

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/04450

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04N 7/167; H04L 9/00; H04K 1/00

US CL : 380/28, 44, 200, 255, 277, 278

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/28, 44, 200, 255, 277, 278

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
www.hotbot.com; www.acm.org; www.ieee.org

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
Please See Continuation Sheet

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|------------|--|-----------------------|
| X          | Billham et al, "A proof of the security of quantum key distribution," 2000, ACM, see section 1.2, pages 717-718                              | 1-7,9                 |
| A          | Zhang et al, "Cryptographically resilient functions," September 1997, IEEE transactions on information theory, Vol. 43, No. 5, see page 1740 | 1-9                   |
| A          | US 5,675,648 A (TOWNSEND) 07 October 1997, see entire document   | 1-9                   |



Further documents are listed in the continuation of Box C.



See patent family annex.

### \* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

20 September 2004 (20.09.2004)

Date of mailing of the international search report

27 SEP 2004

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Facsimile No. (703) 305-3230

Authorized officer

Ayaz Sheikh

Telephone No. 703-305-3900

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/04450

Continuation of B. FIELDS SEARCHED Item 3:  
BRS (files: USPAT, DERWENT, JPO, EPO, IBM TDB, US PG PUB)

search terms: quantum, key, distribution, qkd, stream cipher, random